

Relation between information and disturbance in quantum key distribution protocol with classical Alice

Takayuki Miyadera

Research Center for Information Security,
National Institute of Advanced Industrial Science and Technology,
1-1-1 Umezono, Tsukuba, Ibaraki 305-8561, Japan
miyadera-takayuki@aist.go.jp

The “semiquantum” key distribution protocol introduced by Zou *et al.* is examined. The protocol while using two-way quantum communication requires only Bob to be fully quantum. We derive a trade-off inequality between information gained by Eve and the disturbance observed by legitimate users. It guarantees that Eve cannot obtain large information if the disturbance is sufficiently small.

PACS numbers:

I. INTRODUCTION

Recently, several “semiquantum” key distribution protocols were proposed[1–3]. In contrast to the common quantum key distribution protocols such as BB84, one of the parties in these protocols uses only classical operations. In their pioneering work, Boyer, Kenigsberg and Mor introduced[1] a two-way semiquantum key distribution protocol using four states. Zou, Qiu, Li, Wu, and Li derived[3] its simplification that requires only one state. These protocols are interesting, because they give insights into the necessary conditions for achieving secure communication. In return for the merit that the protocols need only one quantum party, they use two-way quantum communication channels. This makes the security proof difficult. In fact, only the robustness of the protocols has been proved so far[1, 2, 4–6]. The robustness of the protocols suggests that information gained by Eve inevitably disturbs the communication between Alice and Bob. While this robustness is necessary for the security of the protocols, as the no-cloning theorem was in the BB84 protocol, the next important step should be taken for showing a quantitative trade-off relationship between the information gained by Eve and the disturbance observed by legitimate users[7, 8]. This type of relationship in the BB84 protocol is called the information-disturbance theorem[9, 10].

In this paper, we derive such a trade-off relationship in the protocol introduced by Zou *et al.*[3]. In this protocol, the existence of Eve is noticed by performing two error-checking procedures. The inequality we derive relates the amount of information gained by Eve to these error probabilities.

II. FORMULATION AND RESULTS

A. Formulation

The protocol given by Zou *et al.*[3] runs as follows. Bob sends Alice N qubits each in the state $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and keeps all qubits he receives back from her in a quantum memory. After confirming the receipt of all qubits by Bob, Alice publicly announces which qubits she reflected (without disturbing them); Bob then checks that he received $|+\rangle$ and not $|-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ on those positions (CTRL). For the (SIFT) qubits measured by Alice in the standard (classical) $\{|0\rangle, |1\rangle\}$ basis, a sample is chosen to be checked for errors (TEST). The remaining SIFT bits serve for obtaining a final key via error correction and privacy amplification.

Instead of this full protocol, we treat its toy version using a qubit without the public discussion. This protocol including Eve’s attack is described as follows. We consider two situations: CTRL and SIFT. In both situations, Bob first sends a qubit to Alice in the state $|+\rangle \in \mathcal{H} := \mathbf{C}^2$. Eve makes the qubit interact with her apparatus \mathcal{K} by a unitary operation $V : \mathcal{H} \otimes \mathcal{K} \rightarrow \mathcal{H} \otimes \mathcal{K}$. The whole state evolves into

$$|\Psi\rangle := V|+\rangle \otimes |\Omega\rangle,$$

where $|\Omega\rangle$ denotes the initial state of Eve’s apparatus.

In the case of CTRL, Alice reflects the qubit without disturbing it. Eve again makes the qubit sent from Alice to Bob interact with her apparatus. It is described by a unitary operation $U : \mathcal{H} \otimes \mathcal{K} \rightarrow \mathcal{H} \otimes \mathcal{K}$. The whole state after the interaction is thus described as $U|\Psi\rangle = UV|+\rangle \otimes |\Omega\rangle$. Bob measures a projection-valued measure (PVM) $X = \{X_+, X_-\} := \{|+\rangle\langle+| \otimes \mathbf{1}_{\mathcal{K}}, |-\rangle\langle-| \otimes \mathbf{1}_{\mathcal{K}}\}$ to check whether the state is in $|+\rangle$. We define $P_{CTRL} := \langle\Psi|U^*X_-U|\Psi\rangle$, which is an error probability in CTRL.

In the case of SIFT, after receiving a qubit, Alice measures a PVM $Z = \{Z_0, Z_1\} := \{|0\rangle\langle 0| \otimes \mathbf{1}_K, |1\rangle\langle 1| \otimes \mathbf{1}_K\}$. The probability for obtaining $z \in \{0, 1\}$ is calculated as $p_{SIFT}^A(z) := \langle \Psi | Z_z | \Psi \rangle$. The state after the measurement is changed according to the von Neumann-Lüders postulate. If z is obtained, the whole state becomes

$$\sigma_z := \frac{Z_z |\Psi\rangle \langle \Psi| Z_z}{p_{SIFT}^A(z)}.$$

Alice sends the qubit back to Bob. Also in this case, Eve makes the qubit interact with her apparatus by using U . The whole system thus becomes $U\sigma_z U^*$. After receiving the qubit, Bob checks the state by measuring Z . The (conditional) probability for obtaining $z' \in \{0, 1\}$ when Alice's outcome is z is represented as $p_{SIFT}^{B|A}(z'|z) := \text{tr}(U\sigma_z U^* Z_{z'})$. Using these quantities, we define an error probability in SIFT by $P_{SIFT} := p_{SIFT}^{B|A}(1|0)p_{SIFT}^A(0) + p_{SIFT}^{B|A}(0|1)p_{SIFT}^A(1)$. This quantity is represented as $P_{SIFT} = \langle \Psi | Z_0 U^* Z_1 U Z_0 | \Psi \rangle + \langle \Psi | Z_1 U^* Z_0 U Z_1 | \Psi \rangle$. Eve's purpose is to know the outcome obtained by Alice. Let us denote the state possessed by Eve after the two-way quantum communication when Alice obtains z in SIFT by ρ_z . It is represented as

$$\rho_z := \text{tr}_{\mathcal{H}}(U\sigma_z U^*),$$

where $\text{tr}_{\mathcal{H}}$ is the partial trace over \mathcal{H} . Eve measures a positive-operator-valued measure (POVM) $E = \{E_e\}$ which acts only on \mathcal{K} for extracting information. That is, each E_e can be represented as $E_e = \mathbf{1}_{\mathcal{H}} \otimes \hat{E}_e$ by using some \hat{E}_e . We denote by $p_{SIFT}^{E|A}(e|z)$ the probability for obtaining an outcome e when Alice obtains z . It is represented as $p_{SIFT}^{E|A}(e|z) = \text{tr}(\rho_z E_e)$. We denote by $p_{SIFT}^{AE}(z, e)$ the joint probability representing the case that Alice obtains z and Eve obtains e . This quantity is calculated as $p_{SIFT}^{AE}(z, e) = p_{SIFT}^{E|A}(e|z)p_{SIFT}^A(z) = \langle \Psi | Z_z U^* E_e U Z_z | \Psi \rangle$. In addition, the probability for obtaining e is calculated as $p_{SIFT}^E(e) := \sum_z p_{SIFT}^{E|A}(e|z)p_{SIFT}^A(z)$. The information gained by Eve is characterized by the mutual information, which is defined by

$$I(A : E) = H(A) + H(E) - H(A, E),$$

where $H(A) := -\sum_z p_{SIFT}^A(z) \log_2 p_{SIFT}^A(z)$, $H(E) := -\sum_e p_{SIFT}^E(e) \log_2 p_{SIFT}^E(e)$ and $H(A, E) := -\sum_{z,e} p_{SIFT}^{AE}(z, e) \log_2 p_{SIFT}^{AE}(z, e)$. Eve has two chances to make her apparatus interact with the qubit. It is obvious that each interaction can help her obtain information. For instance, Eve can have an entangled state between her apparatus and the qubit sent to Alice by using V . Although it brings her information, this interaction leaves its trace behind by disturbing the state. Our aim in this paper is to derive a trade-off inequality that bounds $I(A : E)$ by P_{CTRL} and P_{SIFT} for general attacks in which both U and V are arbitrary.

B. Relation between information and disturbance

The following is our main theorem.

Theorem 1 *The information gained by Eve can be bounded from above as*

$$I(A : E) \leq 2\sqrt{P_{CTRL} + 6P_{SIFT}^{1/4}},$$

where P_{SIFT} and P_{CTRL} are the error probabilities defined above.

This theorem generalizes the robustness result. In fact, if we put $P_{CTRL} = P_{SIFT} = 0$ in the above inequality, $I(A : E) = 0$ follows. That is, information gained by Eve inevitably causes disturbance. Moreover, the theorem guarantees that information gained by Eve is small if both of the probabilities P_{CTRL} and P_{SIFT} are sufficiently small.

We employ two lemmas to prove our main theorem. The following lemma is employed to bound the mutual information by a quantity that is easier to treat.

Lemma 1 *Let X and Y be random variables. Suppose that X takes a value in $\{0, 1\}$. Denote by $p^{XY}(x, y)$ the joint probability representing the case that X takes x and Y takes y . The mutual information between X and Y is bounded as*

$$I(X : Y) \leq \sqrt{1 - 4 \left(\sum_y p^{XY}(0, y)^{1/2} p^{XY}(1, y)^{1/2} \right)^2}.$$

Proof: The proof is the slightest modification of Theorem 1 in Ref.[11]. Let us denote by $p^X(x)$ and $p^Y(y)$ the marginal probabilities with their apparent notations, and by $p^{X|Y}(x|y)$ the conditional probability defined by $p^{X|Y}(x|y) = \frac{p^{XY}(x,y)}{p^Y(y)}$. The mutual information can be written as

$$I(X : Y) = H(X) - H(X|Y),$$

where $H(X) := -\sum_x p^X(x) \log_2 p^X(x)$ and $H(X|Y) := -\sum_y p^Y(y) \sum_x p^{X|Y}(x|y) \log_2 p^{X|Y}(x|y)$. Because $H(X) \leq 1$ and $-\sum_x p^{X|Y}(x|y) \log_2 p^{X|Y}(x|y) \geq 2 \min\{p^{X|Y}(0|y), p^{X|Y}(1|y)\}$ hold, it holds that

$$I(X : Y) \leq 1 - 2 \sum_y p^Y(y) \min\{p^{X|Y}(0|y), p^{X|Y}(1|y)\}.$$

Using $p^{X|Y}(0|y) + p^{X|Y}(1|y) = 1$, we obtain $-2 \min\{p^{X|Y}(0|y), p^{X|Y}(1|y)\} = -1 + |p^{X|Y}(0|y) - p^{X|Y}(1|y)|$. Thus it holds that

$$I(X : Y) \leq \sum_y p^Y(y) |p^{X|Y}(0|y) - p^{X|Y}(1|y)| = \sum_y |p^{XY}(0, y) - p^{XY}(1, y)|.$$

The right-hand side of this inequality can be bounded as follows:

$$\begin{aligned} & \sum_y |p^{XY}(0, y) - p^{XY}(1, y)| \\ &= \sum_y \left| \sqrt{p^{XY}(0, y)} - \sqrt{p^{XY}(1, y)} \right| \left| \sqrt{p^{XY}(0, y)} + \sqrt{p^{XY}(1, y)} \right| \\ &\leq \left(\sum_y \left(\sqrt{p^{XY}(0, y)} - \sqrt{p^{XY}(1, y)} \right)^2 \sum_y \left(\sqrt{p^{XY}(0, y)} + \sqrt{p^{XY}(1, y)} \right)^2 \right)^{1/2} \\ &= \left(1 - 2 \sum_y p^{XY}(0, y)^{1/2} p^{XY}(1, y)^{1/2} \right)^{1/2} \left(1 + 2 \sum_y p^{XY}(0, y)^{1/2} p^{XY}(1, y)^{1/2} \right)^{1/2} \\ &= \left(1 - 4 \left(\sum_y p^{XY}(0, y)^{1/2} p^{XY}(1, y)^{1/2} \right)^2 \right)^{1/2}, \end{aligned}$$

where we used the Cauchy-Schwarz inequality. ■

The following lemma plays an important role in relating probabilities in SIFT and CTRL with each other.

Lemma 2 For any (possibly unnormalized) vectors $|\phi_0\rangle, |\phi_1\rangle \in \mathcal{H} \otimes \mathcal{K}$, any bounded operator X acting only on \mathcal{H} , any POVM $E = \{E_e\}$ acting only on \mathcal{K} , it holds that

$$|\langle \phi_0 | X | \phi_1 \rangle| \leq \|X\| \sum_e \langle \phi_0 | E_e | \phi_0 \rangle^{1/2} \langle \phi_1 | E_e | \phi_1 \rangle^{1/2}, \quad (1)$$

where $\|\cdot\|$ is an operator norm defined by $\|X\| := \sup_{\phi \neq 0} \frac{\|X|\phi\rangle\|}{\| |\phi\rangle \|}$.

Proof: Using the commutativity between $E_e^{1/2}$ and X , we obtain

$$|\langle \phi_0 | X | \phi_1 \rangle| = \left| \sum_e \langle \phi_0 | X E_e | \phi_1 \rangle \right| = \left| \sum_e \langle \phi_0 | E_e^{1/2} X E_e^{1/2} | \phi_1 \rangle \right|.$$

We further obtain

$$\begin{aligned} |\langle \phi_0 | X | \phi_1 \rangle| &\leq \sum_e |\langle \phi_0 | E_e^{1/2} X E_e^{1/2} | \phi_1 \rangle| \\ &\leq \sum_e \langle \phi_0 | E_e | \phi_0 \rangle^{1/2} \langle \phi_1 | E_e^{1/2} X^* X E_e^{1/2} | \phi_1 \rangle^{1/2} \\ &\leq \sum_e \langle \phi_0 | E_e | \phi_0 \rangle^{1/2} \langle \phi_1 | E_e | \phi_1 \rangle^{1/2} \|X\|, \end{aligned}$$

where we used the Cauchy-Schwarz inequality to derive the second line and the definition of the operator norm to derive the third line. \blacksquare

Proof: (Proof of Theorem 1) We apply Lemma 1 to $p_{SIFT}^{AE}(z, e)$ in order to bound $I(A : E)$. To bound $p_{SIFT}^{AE}(z, e)$ by P_{SIFT} and P_{CTRL} , we compare this quantity with another probability $p_0(z, e)$ defined by $p_0(z, e) := \langle \Psi | U^* Z_z E_e U | \Psi \rangle$. Using $Z_z + Z_{z \oplus 1} = \mathbf{1}$, we obtain

$$\begin{aligned} U Z_z &= Z_z U Z_z + Z_{z \oplus 1} U Z_z \\ &= Z_z U + C_z, \end{aligned}$$

where $C_z := Z_{z \oplus 1} U Z_z - Z_z U Z_{z \oplus 1}$. Thus it holds that

$$\begin{aligned} p_{SIFT}^{AE}(z, e) &= \langle \Psi | (U^* Z_z + C_z^*) E_e (Z_z U + C_z) | \Psi \rangle \\ &= p_0(z, e) + \langle \Psi | U^* Z_z E_e C_z | \Psi \rangle + \langle \Psi | C_z^* Z_z E_e U | \Psi \rangle + \langle \Psi | C_z^* E_e C_z | \Psi \rangle. \end{aligned}$$

We obtain

$$\begin{aligned} |p_{SIFT}^{AE}(z, e) - p_0(z, e)| &= |\langle \Psi | U^* Z_z E_e C_z | \Psi \rangle + \langle \Psi | C_z^* Z_z E_e U | \Psi \rangle + \langle \Psi | C_z^* E_e C_z | \Psi \rangle| \\ &\leq \langle \Psi | U^* Z_z E_e U | \Psi \rangle^{1/2} \langle \Psi | C_z^* E_e C_z | \Psi \rangle^{1/2} + \langle \Psi | C_z^* E_e C_z | \Psi \rangle^{1/2} \langle \Psi | U^* Z_z E_e U | \Psi \rangle^{1/2} \\ &\quad + \langle \Psi | C_z^* E_e C_z | \Psi \rangle \\ &= 2p_0(z, e)^{1/2} \langle \Psi | C_z^* E_e C_z | \Psi \rangle^{1/2} + \langle \Psi | C_z^* E_e C_z | \Psi \rangle, \end{aligned}$$

where we used the triangular inequality and the Cauchy-Schwarz inequality. Because $|a - b| \leq c$ implies $|\sqrt{a} - \sqrt{b}| \leq \sqrt{c}$ for positive a, b and c , it holds that

$$\left| \sqrt{p_{SIFT}^{AE}(z, e)} - \sqrt{p_0(z, e)} \right| \leq \left(2p_0(z, e)^{1/2} \langle \Psi | C_z^* E_e C_z | \Psi \rangle^{1/2} + \langle \Psi | C_z^* E_e C_z | \Psi \rangle \right)^{1/2}. \quad (2)$$

We apply Lemma 2 to $|\phi_0\rangle = Z_0 U |\Psi\rangle$, $|\phi_1\rangle = Z_1 U |\Psi\rangle$ and $X = |0\rangle\langle 1| \otimes \mathbf{1}_K$. The left-hand side of (1) can be bounded as

$$\begin{aligned} |\langle \phi_0 | X | \phi_1 \rangle| &= |\langle \Psi | U^* (|0\rangle\langle 1| \otimes \mathbf{1}_K) U | \Psi \rangle| \\ &\geq \frac{\langle \Psi | U^* (|0\rangle\langle 1| \otimes \mathbf{1}_K) U | \Psi \rangle + \langle \Psi | U^* (|1\rangle\langle 0| \otimes \mathbf{1}_K) U | \Psi \rangle}{2} \\ &= \frac{1}{2} - \langle \Psi | U^* X_- U | \Psi \rangle \\ &= \frac{1}{2} - P_{CTRL}. \end{aligned} \quad (3)$$

The right-hand side of (1) becomes

$$\begin{aligned} \|X\| \sum_e \langle \phi_0 | E_e | \phi_0 \rangle^{1/2} \langle \phi_1 | E_e | \phi_1 \rangle^{1/2} &= \sum_e p_0(0, e)^{1/2} p_0(1, e)^{1/2} \\ &\leq \sum_e \left(p_{SIFT}^{AE}(0, e)^{1/2} + \left(2p_0(0, e)^{1/2} \langle \Psi | C_0^* E_e C_0 | \Psi \rangle^{1/2} + \langle \Psi | C_0^* E_e C_0 | \Psi \rangle \right)^{1/2} \right) \\ &\quad \cdot \left(p_{SIFT}^{AE}(1, e)^{1/2} + \left(2p_0(1, e)^{1/2} \langle \Psi | C_1^* E_e C_1 | \Psi \rangle^{1/2} + \langle \Psi | C_1^* E_e C_1 | \Psi \rangle \right)^{1/2} \right), \end{aligned} \quad (4)$$

where we used (2). By using the Cauchy-Schwarz inequality, we can further bound the above inequality as

$$\begin{aligned}
(4) &\leq \sum_e p_{SIFT}^{AE}(0, e)^{1/2} p_{SIFT}^{AE}(1, e)^{1/2} \\
&+ p_{SIFT}^A(0)^{1/2} \left(\sum_e (2p_0(1, e)^{1/2} \langle \Psi | C_1^* E_e C_1 | \Psi \rangle^{1/2} + \langle \Psi | C_1^* E_e C_1 | \Psi \rangle) \right)^{1/2} \\
&+ p_{SIFT}^A(1)^{1/2} \left(\sum_e (2p_0(0, e)^{1/2} \langle \Psi | C_0^* E_e C_0 | \Psi \rangle^{1/2} + \langle \Psi | C_0^* E_e C_0 | \Psi \rangle) \right)^{1/2} \\
&+ \left(\sum_e (2p_0(1, e)^{1/2} \langle \Psi | C_1^* E_e C_1 | \Psi \rangle^{1/2} + \langle \Psi | C_1^* E_e C_1 | \Psi \rangle) \right)^{1/2} \\
&\times \left(\sum_e (2p_0(0, e)^{1/2} \langle \Psi | C_0^* E_e C_0 | \Psi \rangle^{1/2} + \langle \Psi | C_0^* E_e C_0 | \Psi \rangle) \right)^{1/2}.
\end{aligned}$$

The terms $\sum_e (2p_0(0, e)^{1/2} \langle \Psi | C_0^* E_e C_0 | \Psi \rangle^{1/2} + \langle \Psi | C_0^* E_e C_0 | \Psi \rangle)$ and $\sum_e (2p_0(1, e)^{1/2} \langle \Psi | C_1^* E_e C_1 | \Psi \rangle^{1/2} + \langle \Psi | C_1^* E_e C_1 | \Psi \rangle)$ are bounded as

$$\begin{aligned}
&\sum_e (2p_0(0, e)^{1/2} \langle \Psi | C_0^* E_e C_0 | \Psi \rangle^{1/2} + \langle \Psi | C_0^* E_e C_0 | \Psi \rangle) \\
&\leq 2p_0^A(0)^{1/2} \langle \Psi | C_0^* C_0 | \Psi \rangle^{1/2} + \langle \Psi | C_0^* C_0 | \Psi \rangle \\
&\sum_e (2p_0(1, e)^{1/2} \langle \Psi | C_1^* E_e C_1 | \Psi \rangle^{1/2} + \langle \Psi | C_1^* E_e C_1 | \Psi \rangle) \\
&\leq 2p_0^A(1)^{1/2} \langle \Psi | C_1^* C_1 | \Psi \rangle^{1/2} + \langle \Psi | C_1^* C_1 | \Psi \rangle,
\end{aligned}$$

where $p_0^A(z) := \sum_e p_0(z, e)$ and we used the Cauchy-Schwarz inequality and the relation $\sum_e E_e = \mathbf{1}_K$. Because $C_z^* C_z = Z_z U^* Z_{z \oplus 1} U Z_z + Z_{z \oplus 1} U^* Z_z U Z_{z \oplus 1}$ holds, we have, for $z = 0, 1$,

$$\langle \Psi | C_z^* C_z | \Psi \rangle = P_{SIFT}.$$

Thus we obtain

$$\begin{aligned}
&\|X\| \sum_e \langle \phi_0 | E_e | \phi_0 \rangle^{1/2} \langle \phi_1 | E_e | \phi_1 \rangle^{1/2} \leq \sum_e p_{SIFT}^{AE}(0, e)^{1/2} p_{SIFT}^{AE}(1, e)^{1/2} \\
&+ p_{SIFT}^A(0)^{1/2} (2p_0^A(1)^{1/2} P_{SIFT}^{1/2} + P_{SIFT})^{1/2} \\
&+ p_{SIFT}^A(1)^{1/2} (2p_0^A(0)^{1/2} P_{SIFT}^{1/2} + P_{SIFT})^{1/2} \\
&+ (2p_0^A(1)^{1/2} P_{SIFT}^{1/2} + P_{SIFT})^{1/2} (2p_0^A(0)^{1/2} P_{SIFT}^{1/2} + P_{SIFT})^{1/2}. \\
&\leq \sum_e p_{SIFT}^{AE}(0, e)^{1/2} p_{SIFT}^{AE}(1, e)^{1/2} \\
&+ (2p_0^A(1)^{1/2} P_{SIFT}^{1/2} + 2p_0^A(0)^{1/2} P_{SIFT}^{1/2} + 2P_{SIFT})^{1/2} \\
&+ \frac{1}{2} \left(2p_0^A(1)^{1/2} P_{SIFT}^{1/2} + 2p_0^A(0)^{1/2} P_{SIFT}^{1/2} + 2P_{SIFT} \right),
\end{aligned}$$

where we used the Cauchy-Schwarz inequality again. Because $P_{SIFT} \leq P_{SIFT}^{1/2}$ and $p_0^A(0), p_0^A(1) \leq 1$ hold, it holds that

$$\begin{aligned}
&\|X\| \sum_e \langle \phi_0 | E_e | \phi_0 \rangle^{1/2} \langle \phi_1 | E_e | \phi_1 \rangle^{1/2} \\
&\leq \sum_e p_{SIFT}^{AE}(0, e)^{1/2} p_{SIFT}^{AE}(1, e)^{1/2} + \sqrt{6} P_{SIFT}^{1/4} + 3P_{SIFT}^{1/2} \\
&\leq \sum_e p_{SIFT}^{AE}(0, e)^{1/2} p_{SIFT}^{AE}(1, e)^{1/2} + 6P_{SIFT}^{1/4},
\end{aligned} \tag{5}$$

where we used $\sqrt{6} + 3 < 6$. (Although the above inequality can be slightly improved, we do not treat it here as it is not important.) Thus (3), (5) and Lemma 2 derive

$$\frac{1}{2} - P_{CTRL} - 6P_{SIFT}^{1/4} \leq \sum_e p_{SIFT}^{AE}(0, e)^{1/2} p_{SIFT}^{AE}(1, e)^{1/2}.$$

Now we can apply Lemma 1 to obtain

$$\begin{aligned} I(A : E) &\leq 2\sqrt{(P_{CTRL} + 6P_{SIFT}^{1/4}) - (P_{CTRL} + 6P_{SIFT}^{1/4})^2} \\ &\leq 2\sqrt{P_{CTRL} + 6P_{SIFT}^{1/4}}. \end{aligned}$$

■

III. SUMMARY

In this paper, treating the quantum key distribution protocol with classical Alice, we obtained a trade-off relationship between information gained by Eve and the disturbance observed by Alice and Bob. Our theorem provides a generalization of the robustness result obtained thus far. Moreover it guarantees that information gained by Eve is small if both of two error probabilities observed by the legitimate users are sufficiently small. Applying the inequality to the full protocol in order to examine its security is an important future problem.

Acknowledgments: I would like to thank Prof. Hideki Imai for his encouragements.

-
- [1] M. Boyer, D. Kenigsberg, and T. Mor, *Phys. Rev. Lett.* **99** (2007) 140501.
 - [2] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, *Phys. Rev. A* **79** (2009) 032341.
 - [3] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, *Phys. Rev. A* **79** (2009) 052312.
 - [4] M. Boyer and T. Mor, *Phys. Rev. A* **83** (2011) 046301.
 - [5] X. Zou and D. Qiu, *Phys. Rev. A* **83** (2011) 046302.
 - [6] M. Boyer and T. Mor, arXiv:1012.2418.
 - [7] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, *Journal of cryptology* **19** (2006) 381.
 - [8] M. Hayashi, *Phys. Rev. A* **74** (2006) 022307.
 - [9] P. O. Boykin and V. P. Roychowdhuri, *Quantum Information and Computation* **5** (2005) 596.
 - [10] T. Miyadera and H. Imai, *Phys. Rev. A* **73** (2006) 042317.
 - [11] C. A. Fuchs and J. V. D. Graaf, *IEEE Transactions on Information Theory* **45** (1999) 1216.